REMARKS

Applicant respectfully traverses and requests reconsideration.

Applicant wishes to thank the Examiner for the notice that claims 4, 5, 12, 27, 39, 53, 59, 65, 66, 68, 69, 71, 72, 73 are objected to but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. However, as noted below, Applicant also respectfully submits that the unallowed claims are also in condition for allowance.

Claims 1-11, 19-21, 24, 33-38, 45-47, 50, 60-61, 64, 67 and 70 stand rejected under 35 U.S.C. §102(b) as being anticipated by Fisherman et al. The "Response to Arguments" section of the office action states that "Applicant's arguments with respect to claims 1-73 have been considered but are moot in view of new ground(s) of rejection." (Page 2 of office action). However, it appears that the exact same rejections for all rejected claims were cut and pasted from the previous office action and as such, there does not appear to be any new grounds of rejection presented. If Applicant has misunderstood as to which rejections are new, Applicant respectfully requests that the Examiner point out the new rejections.

Applicant respectfully notes that these same rejections were successfully addressed in the Pre Appeal Brief Request for Review on December 27, 2006. Applicant's arguments were believed to be persuasive since prosecution was reopened in response to the filed remarks. As such, Applicant respectfully submits that the current rejections of the independent claims to the extent they are the exact rejections previously presented, should also be withdrawn as they have been previously overcome.

In any event, as set forth below, the Fisherman reference does not teach what is alleged and is missing claim limitations set forth in the claims and as such, the claims are in condition for allowance.

The Fisherman reference is directed to a personal computer hard disk protection system. The system comprises protection programs that interpret logical drives of the hard disk as a fixed set of zones for a particular user wherein each of the fixed set of zones each has respective access rules. The system includes a hardware module (PPSM) responsive to the protection programs and operable to allow or deny access to the hard disk based on the access rules. Fisherman et al. do not teach or suggest, among other things, determining if an access request is a security risk, then determining the state of a switch, and then determining whether to execute a determined security risk access request based on a determined switch state. Fisherman et al. also do not teach or suggest including in a south bridge a protection engine operable to authenticate an interface control command and to selectively allow or inhibit execution of an interface control command by the interface controller depending on whether or not the source of the interface control command is authentic.

Applicant's claimed invention, as recited in independent Claims 1, 64, and 70, is directed to protecting computer assets from unauthorized access. Applicant claims determining if an interface control command is a security risk and, if so, *then determining the state of a switch.* The interface control command that is identified as security risk is then either inhibited or executed *based on the determined state of the switch* (See, for example, Claim 1, lines 5-11). The cited portion of Fisherman et al. is silent as to determining the state of a switch after an interface control command has been determined to be a security risk and using a switch state to further determine whether to allow or to disallow a hard drive access request or other operation that is known to violate an access rule. If Fisherman et al. detects an access request that violates an access rule, this access operation is simply not performed and an error code is returned. The disposition of the violating access request does not depend on determining a switch state (see, for example, column 6, line 62 through column 7, line 2) after a threatening interface control command has been detected. Therefore, features of Applicant's claimed invention are not taught or suggested by Fisherman et al. Accordingly, independent Claims 1, 64, and 70 are allowable, and the dependent claims add additional novel and non-obvious subject matter and should likewise be allowable.

In addition, Fisherman et al. describes a system that switches on each request. It switches, for example, from an active to a passive mode based on a request. (See for example, column 6 and column 8). Applicant claims a different operation which must be disclosed in its entirety in the cited reference or the claim is in condition for allowance. Since, as noted above, the various limitations of the claims are not disclosed, Applicant respectfully submits that the rejection must be withdrawn.

In addition, other claims are also not disclosed in Fisherman et al. For example, claim 6 requires that determining the state of a switch includes determining the state of a software based switch. However, the cited portion is silent as to any switch. Instead, the cited portion actually refers to a module being switched to a passive mode after it is determined what type of program is attempting to change the status indicating that a key program is active. There is no determining of any state of a switch as claimed after a threat has been detected.

Applicant respectfully submits that the cited portion of Fisherman et al. fails to disclose, inter alia, determining if an interface control command is a security risk, determining a switch state in response to the detected threat, and then determining whether to execute a determined security risk access request based on a determined switch state.

As to independent Claims 33 and 67, these claims are directed to protecting computer assets from unauthorized access. Applicant claims, inter alia, receiving an interface control command in a protection engine *in a south bridge*. The security risk of the interface control command is determined. If the interface control command is determined to be a security risk, then the source of the command is authenticated. An interface control command that is a determined security risk is then inhibited or executed based on whether or not the source of the command is authentic (See, for example, Claim 33, lines 3-10). In Claim 67, Applicant teaches *a south bridge* comprising an interface controller and a protection engine operable to determine if a source of an interface control command is authentic and to selectively allow or inhibit execution of the interface control command by the interface controller depending on whether or not the source of the interface control command is authentic. (See Claim 67, lines 3-11). Most particularly, the cited portion of Fisherman et al. is silent on receiving an interface control command in a protection engine in a south bridge or a south bridge that comprises an interface controller and a protection engine operable to authenticate interface control commands. There is no discussion in Fisherman et al. of a protection engine in a south bridge or of a protection engine and an interface controller in a south bridge. Therefore features of Applicant's claimed invention are not taught or suggested by Fisherman et al. Accordingly, independent Claims 1, 64, and 70 are allowable, and the dependent claims add additional novel and non-obvious subject matter and should likewise be allowable.

Claims 13-17, 28-32, 40-44, and 54-58, stand rejected under 35 U.S.C. 103(a) as being unpatentable over Fisherman et al. in view of Glossary of Information Technology Acronyms and Terms (here within GITAT). In regards to Claims 13-17, 28-32, 40-44, and 54-58, Applicant references the relevant remarks above. The GITAT reference provides cursory definitions of system input-output (I/O) terms. The GITAT reference does not teach or suggest either (1) determining if an access request is a security risk, determining a switch state, and then determining whether to execute a determined security risk access request based on a determined switch state or (2) including in a south bridge a protection engine operable to authenticating interface control commands. Accordingly, the dependent claims add additional novel and non-obvious subject matter and should be allowable.

Claims 18, 25, 26, 51, and 52, stand rejected under 35 U.S.C. 103(a) as being unpatentable over Fisherman et al. and GITAT as applied to Claims 1 and 13 above, and further in view of Davis (USP 6,205,547). In regards to Claims 18, 25, 26, 51, and 52, Applicant references the relevant remarks above. Davis is directed to a computer managing system. However, Davis does not teach or suggest either (1) determining if an access request is a security risk and then determining whether to execute the access request based on a switch state or (2) including in a south bridge a protection engine operable to authenticating an interface control command and to selectively allow or inhibit execution of the interface control command by the interface controller depending on whether or not the source of the interface control command is authentic. Accordingly, the dependent claims add additional novel and non-obvious subject matter and should be allowable.

Claims 22, 23, 48, and 49, stand rejected under 35 U.S.C. 103(a) as being unpatentable over Fisherman et al. in view of Chen et al. (USP 5,832,208). In regards to Claims 22, 23, 48, and 49, Applicant references the relevant remarks above. Chen et al. is directed to an anti-virus software agent. However, Chen et al. do not teach or suggest either (1) determining if an access request is a security risk and then determining whether to execute the access request based on a switch state or (2) including in a south bridge a protection engine operable to authenticating an interface control command and to selectively allow or inhibit execution of the interface control command by the interface controller depending on whether or not the source of the interface control command is authentic. Accordingly, the dependent claims add additional novel and non-obvious subject matter and should be allowable.

Claims 62 and 63 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Fisherman et al. in view of Applied Cryptography 2"d Edition (here within AC). In regards to Claims 62 and 63, Applicant references the relevant remarks above. AC is directed to an anti-virus software agent. However, AC does not teach or suggest either (1) determining if an access request is a security risk and then determining whether to execute the access request based on a switch state or (2) including in a south bridge a protection engine operable to authenticating an interface control command and to selectively allow or inhibit execution of the interface control command by the interface controller depending on whether or not the source of the interface control command is authentic. Accordingly, the dependent claims add additional novel and non-obvious subject matter and should be allowable.

Accordingly, Applicant respectfully submits that the claims are in condition for allowance and that a timely Notice of Allowance be issued in this case. The Examiner is invited to contact the below-listed attorney if the Examiner believes that a telephone conference will advance the prosecution of this application.

Respectfully submitted,

Date: 7-6-07

By: Chris Reckamp
Christopher J. Reckamp
Registration No. 34,414

Vedder, Price, Kaufman & Kammholz, P.C.
222 N. LaSalle Street
Chicago, IL 60601
(312) 609-7500
FAX: (312) 609-5005